E-mail rastreado

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	4 MB
E-mail Remetente	**Hash da Mensagem**
rsidinei@gmail.com	633ea376d7ae1bb6cf98b8f46fc127c4

Data de Envio	Assunto do E-mail	Anexos
11/09/2025 21:23:44	DESCRIÇÃO DA FATURA CIDDEN COM REFERÊNCIA AO	Contém anexos

Evidências do Destinatário: conselho@gaspar.sc.gov.br

Data/Hora Processamento	Evidência
11/09/2025 21:23:59	Entrega ao Servidor de email iCarta.
11/09/2025 21:23:59	Hash da mensagem iCarta: 633ea376d7ae1bb6cf98b8f46fc127c4
11/09/2025 21:23:59	Hash da mensagem iCarta do destinatário: fb770883f308c3d47f709fc6b10dfd2e .
11/09/2025 21:24:00	Assinatura DKIM: a=rsa-sha256; b=Gm3wkTWU1QwmnCRmKkXgLsDaA9wZ/YMVvtN3NPpwhn1d0IfkWipE05CBxYFza9f HgmhAX8SAoJZzf0j2D1E6rw7trF8e2+EkmvLP0rM6IV9Mwj6l7NuSWP1JxCwPGn4CXio6 e8DtFnAw8G5r4yy/AnHfMY+TGxM1aQdf18V/em0=; s=dkim; c=relaxed/relaxed; d=icarta.pro; v=1; bh=ORc9zPMfUVOvY2JlwPU3hqCqF1XN7Q1xeS9VefATLFY=; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding; .
11/09/2025 21:24:01	Aposição do Carimbo do Tempo (PLURIO), HLB(Hora Legal Brasileira): 11/09/2025 21:24:01.0 HLB GMT-03:00 destinatário: conselho@gaspar.sc.gov.br
11/09/2025 21:24:01	Processo finalizado para o envio ao destinátario conselho@gaspar.sc.gov.br .
11/09/2025 21:24:15	Início da tentativa de entrega às 2025-09-11 21:24:04 DEBUG: getProvider() returning javax.mail.Provider[TRANSPORT,smtp,com.sun.mail.smtp.SMTPTransport,Oracle] DEBUG SMTP: useEhlo true, useAuth false DEBUG SMTP: trying to connect to host "186.250.184.4", port 25, isSSL false 220-emailserver.gaspar.sc.gov.br ESMTP Postfix 220 emailserver.gaspar.sc.gov.br ESMTP Postfix DEBUG SMTP: connected to host "186.250.184.4", port: 25 EHLO smtp1.icarta.pro 250-emailserver.gaspar.sc.gov.br 250-PIPELINING 250-SIZE 20480000 250-VRFY 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN DEBUG SMTP: Found extension "PIPELINING", arg "" DEBUG SMTP: Found extension "SIZE", arg "20480000" DEBUG SMTP: Found extension "VRFY", arg "" DEBUG SMTP: Found extension "ETRN", arg "" DEBUG SMTP: Found extension "STARTTLS", arg "" DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg "" DEBUG SMTP: Found extension "8BITMIME", arg "" DEBUG SMTP: Found extension "DSN", arg "" STARTTLS 220 2.0.0 Ready to start TLS EHLO smtp1.icarta.pro 250-emailserver.gaspar.sc.gov.br 250-PIPELINING 250-SIZE 20480000 250-VRFY 250-ETRN 250-AUTH LOGIN PLAIN

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	4 MB
E-mail Remetente	**Hash da Mensagem**
rsidinei@gmail.com	633ea376d7ae1bb6cf98b8f46fc127c4

Data de Envio	Assunto do E-mail	Anexos
11/09/2025 21:23:44	DESCRIÇÃO DA FATURA CIDDEN COM REFERÊNCIA AO	Contém anexos

250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
DEBUG SMTP: Found extension "PIPELINING", arg ""
DEBUG SMTP: Found extension "SIZE", arg "20480000"
DEBUG SMTP: Found extension "VRFY", arg ""
DEBUG SMTP: Found extension "ETRN", arg ""
DEBUG SMTP: Found extension "AUTH", arg "LOGIN PLAIN"
DEBUG SMTP: Found extension "AUTH=LOGIN", arg "PLAIN"
DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg ""
DEBUG SMTP: Found extension "8BITMIME", arg ""
DEBUG SMTP: Found extension "DSN", arg ""
DEBUG SMTP: use8bit true
DEBUG SMTP: found an 8bit part
DEBUG SMTP: found an 8bit part
MAIL FROM:<0ba3b130-7050-4532-a9e2-85d897cfe599-pid@icarta.pro>
250 2.1.0 Ok
DEBUG SMTP: sendPartial set
RCPT TO:<conselho@gaspar.sc.gov.br>
250 2.1.5 Ok
DEBUG SMTP: Verified Addresses
DEBUG SMTP: conselho@gaspar.sc.gov.br
DATA
354 End data with <CR><LF>.<CR><LF>
.
250 2.0.0 Ok: queued as 4EA88420DFB
DEBUG SMTP: message successfully delivered to mail server
QUIT
221 2.0.0 Bye

Mensagem entregue às 2025-09-11 21:24:15
.

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.